Siddharth Pandya

sppandya0907@gmail.com

+91 9619195686

Navi Mumbai, India

https://www.linkedin.com/in/siddharthpandya07/

https://cyberpands.medium.com

https://github.com/cyber-pands

SUMMARY

Cybersecurity professional with an MSc in Cybersecurity and hands-on experience in threat detection, SIEM monitoring, and web application security. Skilled in Splunk, Python Automation, Log Analysis, and OWASP with certifications including Security+ and CySA+. I bring a strong analytical mindset, clear problem-solving ability, and a continuous learning approach focused on improving detection quality, strengthening defenses, and delivering reliable value to a security team.

SKILLS

- Threat Detection
- Log Analysis
- Splunk / Wazuh
- Zeek
- Wireshark
- Linux
- Network Monitoring
- Team building
- Incident Response
- Identity and Access Management (IAM)
- Security Information and Event Management
- Python
- Firewalls
- Windows
- OWASP
- Adaptibility

EXPERIENCE

TEAM LEAD, McDonald's 06/2023 – 11/2025 | United Kingdom

- **Led** a team of five to seven crew members to maintain smooth shift operations, improving workflow accuracy and service consistency, and strengthening my attention to detail and process discipline.
- **Monitored** POS systems, order screens, and dashboards to spot irregularities, reducing transaction errors and maintaining data accuracy, which improved my ability to detect anomalies early.
- **Trained** new staff on correct and safe use of digital tools, decreasing operational mistakes and improving team efficiency, while enhancing my communication and coaching skills.
- **Managed** daily stock checks and digital inventory updates, reducing discrepancies and improving record integrity, reinforcing the importance of accurate data handling.
- **Resolved** customer issues and documented incidents clearly, ensuring smooth escalations and improving service quality, which strengthened my structured incident-handling approach.
- **Collaborated** with supervisors to report equipment faults and workflow bottlenecks, supporting quick resolution and minimizing disruption, and developing better risk awareness and escalation judgment.

CYBERSECURITY RESEARCHER, Nybble IT 05/2022 – 10/2022 | United Kingdom

- **Analyzed** web payment security protocols and presented findings at the GM Chamber, improving client awareness and adoption of stronger encryption practices, which strengthened my ability to communicate complex security concepts clearly.

- **Conducted** vulnerability assessments using automated tools and manual testing, identifying key weaknesses and contributing to more secure system configurations, enhancing my practical understanding of offensive and defensive techniques.
- **Developed** incident response strategies for simulated attacks, reducing recovery time and improving response readiness, while deepening my knowledge of structured IR workflows.
- **Collaborated** with developers and technical teams to apply security improvements, enhancing system resilience against external threats, and reinforcing my cross-team communication and secure design mindset.
- **Documented** security findings and recommended controls, supporting informed decision making and compliance efforts, which improved my ability to produce clear, actionable reports.

PROJECTS

Wazuh SIEM Home Lab
Designed and implemented a Wazuh SIEM security monitoring lab leveraging AWS EC2 and virtual endpoints, demonstrating proficiency in real-time threat detection, file integrity monitoring, and security event analysis across multiple operating systems.

PCAPThreatHunter
Created a Python tool to automate the extraction of Indicators of Compromise (IOCs) from Zeek logs and match them with open-source threat intelligence platforms including AbuseIPDB, AlienVault, and Abuse.ch.

SecureGuard
Developed a Linux-based automated solution for endpoint protection, vulnerability detection, and real-time security monitoring, significantly reducing manual analyst workload.

Auto-Recon
Engineered an automated reconnaissance utility using Python and Nmap to streamline vulnerability assessments and reduce scan time during penetration testing activities.

CERTIFICATIONS

Splunk Core Certified User 01/04/2025

CompTIA CYSA+ 01/12/2024

CompTIA Security+ 01/09/2024

EDUCATION

MSc, Cybersecurity, Lancaster University 09/2021 – 09/2022 | United Kingdom
- **Completed** an NCSC-certified master's program with hands-on work in threat detection, incident response, and secure system design, strengthening my technical foundation and ability to analyse and defend against evolving cyber threats.

Bachelor of Engineering, Computer Engineering, 08/2016 – 11/2020 | India
Pillai College of Engineering
- **Studied** core computing principles including networking, programming, and system architecture, building the analytical and technical base that supports my cybersecurity problem-solving and tool proficiency.

LANGUAGES

- English
- Hindi
- Marathi
- Gujarati